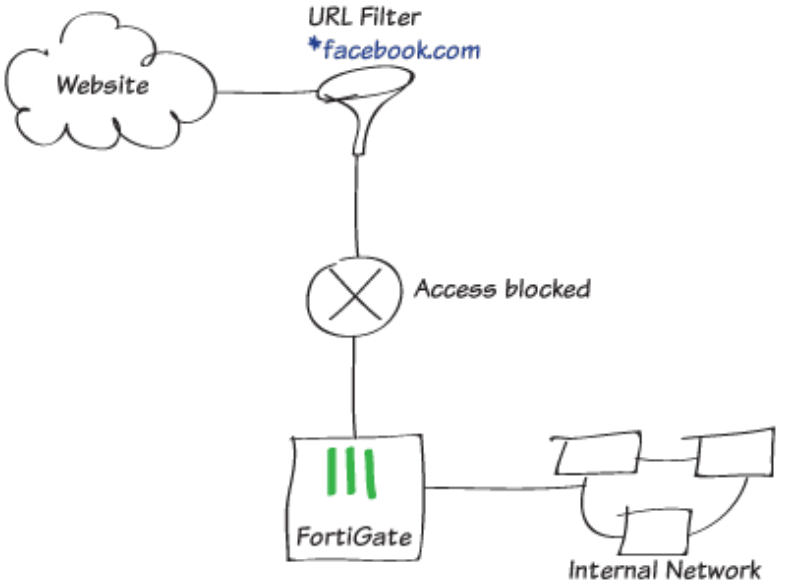
Using a static URL filter to block access to a specific website

When you allow access to a particular type of content, such as the FortiGuard Social Networking category, there may still be certain websites in that category that you wish to prohibit. In this example, you will learn how to configure a FortiGate to prevent access to a specific social networking website, including its subdomains, by means of a static URL filter. And by using SSL inspection, you ensure that this website is also blocked when accessed through HTTPS protocol.

This example uses IPv4 security policies, but this method also works with IPv6 policies. Simply substitute any IPv4 configurations with IPv6 configurations.

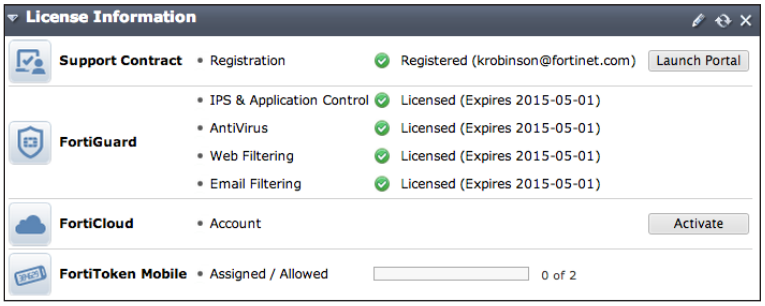
1. Verifying FortiGuard Services subscription
2. Editing the Web FIter profile
3. Verifying the SSL inspection profile
4. Creating a security policy
5. Results



1. Verifying FortiGuard Services subscription

Go to **System** > **Dashboard** > **Status**.

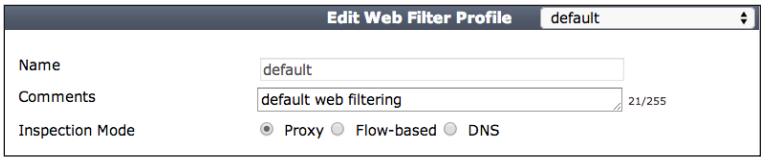
In the **License Information** widget, verify that you have an active subscription to FortiGuard Web Filtering. If you have a subscription, the service will have a green checkmark beside it.



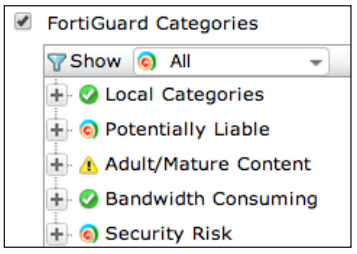
2. Editing the Web Filter profile

Go to **Security Profiles** > **Web Filter** and edit the default Web Filter profile.

Set **Inspection Mode** to **Proxy**.

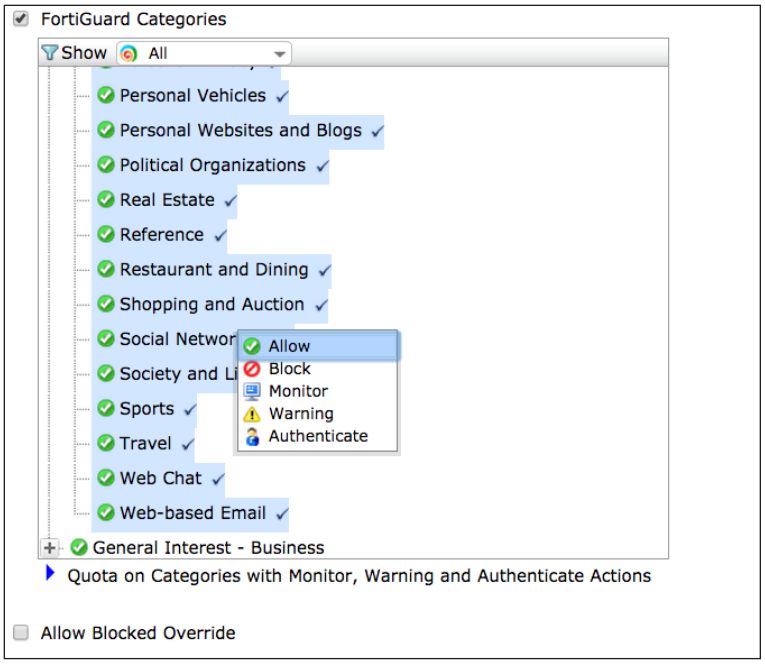


Enable the **FortiGuard Categories** that allow, block, monitor, warn, or authenticate depending on the type of content.

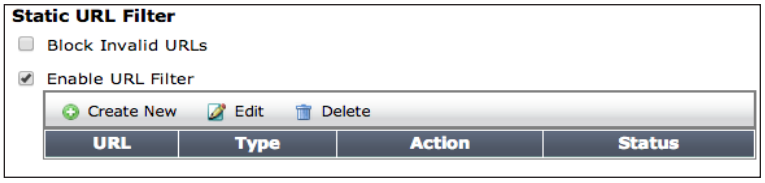


Learn more about FortiGuard Categories at the FortiGuard Center web filtering rating page: www.fortiguard.com/static/webfiltering.html

Under FortiGuard Categories, go to **General Interest - Personal**. Right-click on the **Social Networking** subcategory and ensure it is set to **Allow**.

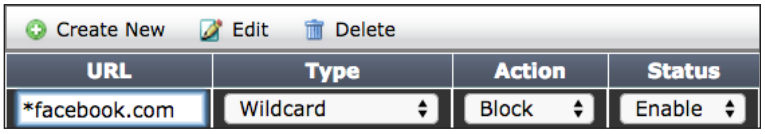


To prohibit visiting one particular social networking site in that category, go to **Static URL Filter**, select **Enable URL Filter**, and then click **Create New**.



For your new web filter, enter the URL of the website you are attempting to block. If you want to block all of the subdomains for that website, omit the protocol in the URL and enter an asterisk (*). For this example, enter:

```
*facebook.com
```



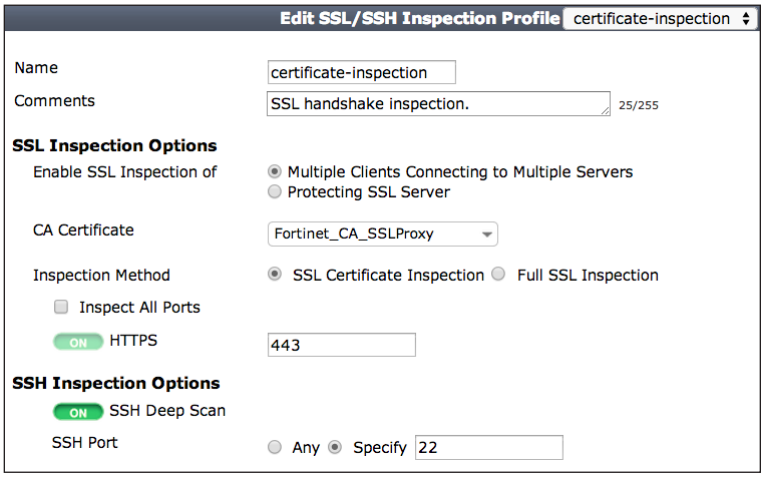
Set **Type** to **Wildcard**, set **Action** to **Block**, and set **Status** to **Enable**.

3. Verifying the SSL inspection profile

Go to **Policy & Objects > Policy > SSL Inspection** and edit the **certificate-inspection** profile.

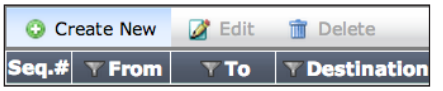
Ensure that **CA Certificate** is set to the default **Fortinet_CA_SSLProxy**.

Ensure **Inspection Method** is set to **SSL Certificate Inspection** and **SSH Deep Scan** is set to **ON**.



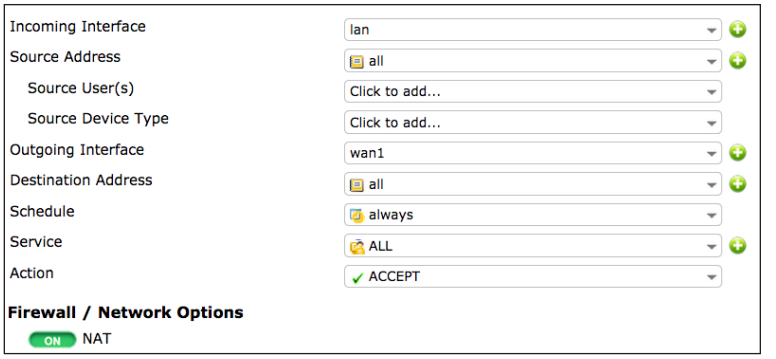
4. Creating a security policy

Go to **Policy & Objects > Policy > IPv4**, and click **Create New**.

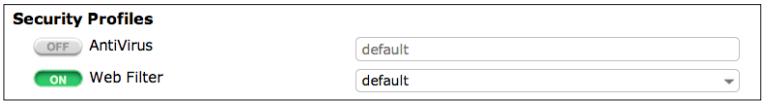


Set the **Incoming Interface** to allow packets from your internal network and set the **Outgoing Interface** to proceed to the Internet-facing interface (typically **wan1**).

Enable **NAT**.

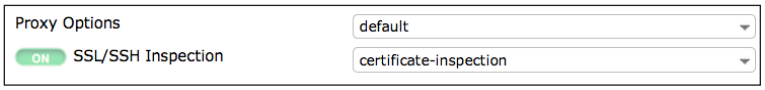


Under **Security Profiles,** enable **Web Filter** and select the **default** web filter.

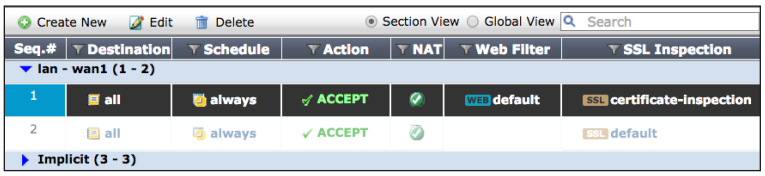


This automatically enables **SSL/SSH Inspection**.

Select **certificate-inspection** from the dropdown menu.



After you have created your new policy, ensure that it is at the top of the policy list. To move your policy up or down, click and drag the far left column of the policy.



5. Results

Visit the following sites to verify that your web filter is blocking websites ending in facebook.com:

- facebook.com
- attachments.facebook.com
- upload.facebook.com
- camdencc.facebook.com
- mariancollege.facebook.com

A FortiGuard **Web Page Blocked!** page should appear.

Visit https://www.facebook.com to verify that HTTPS protocol is blocked. A **Web Page Blocked!** page should appear.